Secure housing containing a keyboard for inserting confidential data

Field of the invention

The present invention relates to a secure housing containing a keyboard for entering confidential data, such as a personal identification number, which are intended in particular for an electronic payment system.

Electronic circuits have contributed greatly to the development of modern companies and are used in numerous fields of technology.

These circuits have in particular permitted the creation and development of so-called "electronic payment" systems which enable various transactions to be carried out from electronic payment terminals equipped with numerical keyboards by using credit cards.

These systems must be rendered secure in order to protect both clients and tradesmen by avoiding any risk of fraudulent transaction.

To that end, banks and manufacturers of credit cards allocate to the latter personal identification numbers which their owners must enter in the numerical keyboard with which electronic payment terminals are equipped.

After they have been entered, the identification numbers as well as other confidential data appearing on credit cards are encrypted in security modules prior to the transaction.

The personal identification number therefore makes it possible to verify that the credit card is indeed being used by its true owner and not by an intruder who has found or stolen it.

For obvious security reasons, it is essential that, between its entry into the numerical keyboard of an electronic payment terminal and its encryption, a personal identification number should not be accessible to ill-intentioned third parties.

It is therefore necessary to associate protective devices with the keyboards.

Fraudsters, however, are proving to be increasingly clever in their attempts to obtain confidential data and therefore it is becoming increasingly difficult to render secure the numerical keyboards of electronic payment terminals.

By way of example, fraudsters can:

- display the acquisition of a confidential code (directly or by way of video systems);
- gain access to the system's electronics, in particular by inserting an electronic "sniffer" card into the system;
- "listen" to the electromagnetic emissions emitted by the system's electronics in order to correlate them with the keys pressed;
- steal information when it is keyed in, for example by placing a false keyboard over the real keyboard, or by spreading over the keyboard a substance, such as dust, which leaves traces on the keys used.

Prior art

Various means have already been proposed for attempting to render secure the numerical keyboards of electronic payment terminals.

By way of example, it has already been proposed to conceal the keys of the keyboards from prying eyes (document WO 00/68859) or to change the position of the keys each time they are used (document WO 98/27518).

Those various means make it more difficult to determine confidential data by watching a user keying them in on a numerical keyboard.

It has also already been proposed to enclose the keyboard, its controller and also the security module associated therewith in a sealed housing in order to prevent fraudsters from gaining access to the electronic system upstream of the encryption of the confidential data entered into the keyboard.

By way of example, it has already been proposed in accordance with the document WO 01/92349 to enclose the electronics between the keyboard and a glass plate.

However, such solutions prove to be very expensive and particularly difficult to implement.

Consequently, there has hitherto been no proposal for a reliable and economically satisfactory means for rendering secure the numerical keyboards of electronic payment system terminals.

Object of the invention

The object of the present invention is to fill this gap by proposing a secure housing containing a numerical keyboard arranged in such a manner as to prevent intruders from gaining fraudulent access to the confidential data entered before the encryption thereof by a security module.

The object of the invention is in particular to detect a device placed on the keyboard in order to determine the confidential data entered, or to prevent any alteration to the system effected for the same purpose.

A further object of the invention is to make it impossible to listen to the electromagnetic emissions generated by the system's electronics.

The housing to which the invention relates is very specially suited to rendering secure the numerical keyboards with which the payment terminals of electronic payment systems are equipped but can be adapted to rendering secure any system in which confidential data are transmitted by keyboard.

Statement of invention

The present invention therefore relates to a secure housing permitting the entry of confidential data, such as a personal identification number which is intended in particular for an electronic payment system, and comprising a capacitive touch matrix which, on the one hand, is connected by connecting wires to a printed circuit board carrying an

associated controller, a security module and electronics sensitive to the variations in the capacitance of the system, and which, on the other hand, is sandwiched between two glass plates, namely a front glass plate or protective plate, and a rear glass plate or support plate.

Such a housing therefore enables the properties of capacitive touch screens, which are well known to the person skilled in the art, to be used to detect the presence of an external device secured to the numerical keyboard, such as, for example, a false keyboard or a substance which has been deposited in order to mark the keys pressed down during the acquisition of the confidential code.

The numerical keyboard is displayed below the glass plates by any suitable device, such as an LCD, CRT, LED, self-adhesive screen, ... and is read by transparency.

In order to enter his confidential code, the user touches with his fingers the protective plate beneath which the keyboard is displayed.

The consequence of this manipulation is to change the capacitance of the system locally, which enables the controller to know the position touched and therefore to determine the confidential code entered.

This is the conventional operation of a capacitive touch screen.

In order to enable the security system to operate satisfactorily, it is of course necessary to have determined in a preliminary calibration step, carried out during the manufacture of the housing, the capacitance of the system at rest ("at rest" meaning that there is no object next to or on the touch screen) at the various locations of the protective plate corresponding to the various keys of the keyboard.

The list of those capacitance values is recorded in a memory as a reference.

Any attempt to "mask" the keyboard for fraudulent purposes modifies the capacitance of the system.

Consequently, in the course of operation, the real capacitance values are constantly compared with the recorded values and any deviation greater than a predetermined authorised level of deviation is interpreted as indicating a fraud and triggers an alarm or the stoppage of the system.

The secure housing to which the invention relates is characterized in that the protective plate is produced from fragmentable glass and is equipped with an electrical conductor constituted by a long wire coupled thereto or by metallization in the form of a loop.

This electrical conductor, on the one hand, forms part of a fraud-detection circuit comprising a voltage source and also a current detector associated with an alarm member and, on the other hand, breaks under the effect of a fragmentation of the protective plate to bring about the interruption of the current in the fraud-detection circuit and the activation of the alarm member.

According to the invention, the fragmentable glass is preferably constituted by tempered glass which shatters into a multitude of fragments in response to impact.

According to a further feature of the invention, the support plate too is produced from fragmentable glass and equipped with an electrical conductor which forms part of the fraud-detection circuit and which breaks under the effect of a fragmentation of the plate to bring about the interruption of the current in the fraud-detection circuit and the activation of the alarm member.

According to the invention, it is also possible to add to the housing a third glass plate or cover plate which covers the support plate on its rear face and which extends to cover the rear face of the printed circuit board.

The presence of that cover plate improves the security of the printed circuit board.

The cover plate too may advantageously be produced from fragmentable glass and equipped with an electrical conductor which forms part of the fraud-detection circuit and which breaks under the effect of a

fragmentation of the plate to bring about the interruption of the current in the fraud-detection circuit and the activation of the alarm member.

Bearing in mind the above-mentioned features, any attempt to gain access to the sensitive parts of the secure housing (security module, for example) brings about the fragmentation of the glass plates and consequently the breakage of a conductor, which is immediately detected by the current-detector and interrupts the power supply to a memory for saving keyboard operating parameters stored during manufacture.

The detection of that breakage triggers an alarm and advantageously the deactivation of the system.

According to a further feature of the invention, the printed circuit board is located in the immediate vicinity of the capacitive touch matrix covered by the protective plate.

That feature enables the connecting wires of the capacitive touch matrix and of the printed circuit board to be as short as possible, the result of which is to prevent access to the circuit through which non-secure confidential data pass.

According to a further feature of the invention, the printed circuit board and the electronic components secured thereto are embedded in a brittle resin, especially an epoxy resin.

That feature ensures that the wires connecting the various electronic components are automatically shattered in the case of physical attack, in particular an attempt to "punch holes" in the glass plates.

The configuration of the secure housing according to the invention therefore prevents an intruder from gaining access to non-secure confidential data downstream of the protective plate.

For the consequence of any attempt to gain access would be to break the various glass plates and/or the brittle resin in which the printed circuit board is embedded, and therefore to damage the system's electronics and destroy the confidential data contained therein.

According to a further, particularly advantageous, feature of the invention, the fraud-detection circuit is passed through by a current oscillating at high frequency and modulated in amplitude and frequency in order to scramble the electromagnetic emissions of the system with respect to the outside and thus to prevent any attempt to read the internal signals of the system by means of an external high-frequency receiver.

According to the invention, it is also possible to provide other means for rendering the housing secure, for example, to associate with the screen a standard optical filter known per se in order to reduce the angle of vision at which the keyboard can be read.

Drawings

The features of the secure housing to which the invention relates will be described in more detail with reference to the appended drawings in which:

- Figure 1 is an exploded diagrammatic perspective view illustrating the configuration of the secure housing;
- Figure 1a is a diagram illustrating the method of using the housing;
- Figure 1b is a diagram illustrating an attempt at fraud;
- Figure 2 is a diagram representing the fraud-detection circuit.

Description of embodiments

According to Figure 1, the secure housing 1 comprises a capacitive touch matrix sandwiched between two plates produced from brittle glass, namely a protective plate 3 and a support plate 5.

The capacitive touch matrix 2 is connected by connecting wires 6 to a printed circuit board 7 carrying the associated controller, a security module 16 (Figure 2) and also electronics sensitive to the variations in the capacitance of the system.

The printed circuit board 7 and the electronic components secured thereto are embedded in a brittle epoxy resin 8.

As shown in Figure 1, the printed circuit board 7 is located in the immediate vicinity of the capacitive touch matrix 2 covered by the protective plate 3 whose length is greater than that of the support plate 5.

The support plate 5 may, if necessary, be covered on its rear face remote from the protective plate 3 by a third glass plate which is not shown in the Figures, namely a cover plate which extends to cover the rear face of the printed circuit board 7.

That configuration permits the maximum possible reduction of the path travelled by non-secure confidential data after they have been entered in the housing 1.

For, at the output of the housing 1, those data have undergone encryption preventing them from being intercepted by a fraudster.

It should be noted that, according to the embodiment shown in the Figures, the touch matrix operates in accordance with the conventional technology of projected capacitive touch screens.

Consequently, the touch matrix is constituted by a matrix of fine microwires connected to the controller.

An oscillation frequency is assigned to each of those microwires.

According to Figure 1a, during normal use, the user touches with his fingers the protective plate 3 through which the keyboard is displayed by a display device 4.

The fact of touching the protective plate 3 modifies the oscillation frequency of the microwires located at the corresponding site.

That modification, which is a function of the system's capacitance, enables the controller secured to the printed circuit board 7 to determine at what site the protective plate 3, and consequently the projected screen, has been touched by the user, and therefore to determine the confidential code entered.

In a preliminary calibration step, the capacitance at rest was measured at each intersection of wires of the touch matrix 7.

The list of values so measured is recorded as a reference in a memory 9 associated with the security module 16 in a manner shown diagrammatically in Figure 2.

According to Figure 1b, if an intruder applies to the protective plate 3 a "marking" device 10, such as a false keyboard or a layer of dust for fraudulent purposes, the real capacitance of the system is modified and that modification is noticed by the control electronics which can generate an alarm or stop the system in response.

It will be appreciated that the invention could be applied to numerous other capacitive touch screen technologies without thereby departing from the scope thereof.

According to Figure 2, the housing 1 also contains a fraud-detection circuit 11 basically comprising a voltage source 12 and also an electrical conductor in the form of a loop 13 coupled to the protective plate 3.

The circuit 11 also contains a current detector 14 associated with an alarm member (not shown).

An attempt to gain access to the sensitive parts of the housing, in particular the printed circuit board 7, results in the breakage of the protective plate 3 and consequently the breakage of the conductor 13, thus bringing about the emission of an alarm, and also the deactivation of the system owing to the erasure of the memory 9.

According to Figure 2, the fraud-detection circuit 11 is also equipped with a protective device 15 enabling the circuit to be supplied with a current oscillating at high frequency and modulated in amplitude and frequency in order to scramble the electromagnetic emissions of the system with respect to the outside.